CA IM Provisioning Server TLS

TLS Infrastructure

PROCESS TO SYNC TLS CERTS FOR
IMPS, IMPM, IMPD

Alan Baugher
CA Sr. Principal Architect

HOW TO UPDATE THE TLS CERTS IN YOUR IMPS ENVIRONMENT 1 of 2

Background: The Identity Manager Provisioning Server (IMPS) provides a certificate management mechanism, which allows administrators to generate self-signed root CA certificate, client, and server certificates.

Step 0: Review this deck and the readme file under C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt

Step 1: Backup the following folders

IMPS Server(s): ~Identity Manager\Provisioning Server\data\tls\ (assumes IMPS and CCS services are installed together)
IMPD Server(s): DXHOME\dxserver\config\
IMPM Gui : ~Identity Manager\Provisioning Manager\data\tls\

Step 2: Select a single IMPS server to generate ALL certificates from.

Step 3: RDP (assumes Win OS) and open Command Line shell (as Administrator)

Step 4: cd C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt

Step 5: Review etassl.conf and if FIPS 140-2 mode is to be enabled/required. If no changes, proceed.
-enable_fips_mode.bat - enables FIPS 140-2 mode [Skip if not needed/required]
-disable_fips_mode.bat - disables FIPS 140-2 mode [Skip if not needed/required]

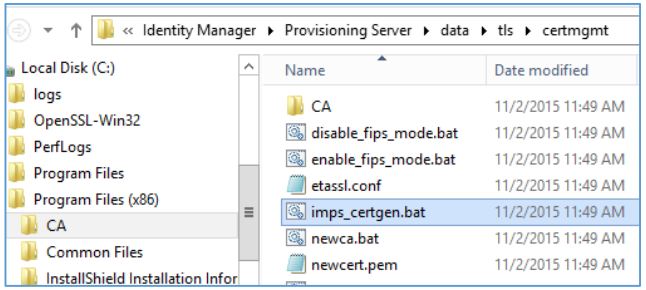
Step 6: Execute **imps_certgen.bat** utility to generate Identity Manager Provisioning Server certificates.
- Continue to hit <enter> 26 times until the utility completes

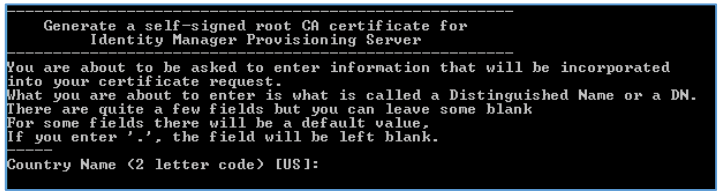
Step 7: After execution, cd to **..\certmgmt\data\tls** sub-folder.

Step 8: Copy the CA Public Cert files per notes in the readme.txt file [IMPS, IMPM, IMPD]

copy ~certmgmt\data\tls**et2_cacert.pem** to ~Identity Manager\Provisioning Server\data\tls**et2_cacert.pem**
copy ~certmgmt\data\tls**et2_cacert.pem** to ~Identity Manager\Provisioning Manager\data\tls**et2_cacert.pem**
copy ~certmgmt\data\tls**et2_cacert.pem** to ~DXHOME\dxserver\config\ssld**\impd_trusted.pem**

Note: If older system replace **etrustadmin_trusted.pem** with **et2_cacert.pem**





ALTERNATIVELY
copy & replace OOTB certs
from latest release of IM:
IMPS/IMPD/IMPM

ca_imps_impm.7z

Use 7zip to extract

HOW TO UPDATE THE TLS CERTS IN YOUR IMPS ENVIRONMENT 1 of 2

Step 9: Copy the Public & RSA Server Cert Files per notes in the readme.txt file

copy ~certmgmt\data\tls\server**eta2_servercert.pem** to ~Identity Manager\Provisioning Server\data\tls\server**eta2_servercert.pem**
copy ~certmgmt\data\tls\server**eta2_serverkey.pem** to ~Identity Manager\Provisioning Server\data\tls\server**eta2_serverkey.pem**

join **eta2_servercert.pem** AND **eta2_serverkey.pem** to new file **IMPD_DSA.pem** {copy –n – paste together; see screen shot example}

copy ~certmgmt\data\tls\server**IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities**HOSTNAME-impd-main.pem**
copy ~certmgmt\data\tls\server**IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities**HOSTNAME-impd-co.pem**
copy ~certmgmt\data\tls\server**IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities**HOSTNAME-impd-inc.pem**
copy ~certmgmt\data\tls\server**IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities**HOSTNAME-impd-notify.pem**
copy ~certmgmt\data\tls\server**IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities**HOSTNAME-imps-router.pem**

Note: If older system with different personalities names; replace the personalities with IMPD_DSA.pem file, e.g. etrustadmin.dxc.pem, etrustadmintemp.pem, etrust_ops.pem

Step 10: Copy the Public and RSA Client Cert Files per notes in the readme.txt

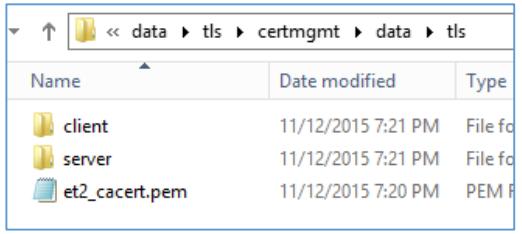
copy ~certmgmt\data\tls\client**eta2_clientcert.pem** to ~Identity Manager\Provisioning Server\data\tls\client**eta2_clientcert.pem**
copy ~certmgmt\data\tls\client**eta2_clientkey.pem** to ~Identity Manager\Provisioning Server\data\tls\client**eta2_clientkey.pem**
copy ~certmgmt\data\tls\client**eta2_clientcert.pem** to ~Identity Manager\Provisioning Manager\data\tls\client**eta2_clientcert.pem**
copy ~certmgmt\data\tls\client**eta2_clientkey.pem** to ~Identity Manager\Provisioning Manager\data\tls\client**eta2_clientkey.pem**

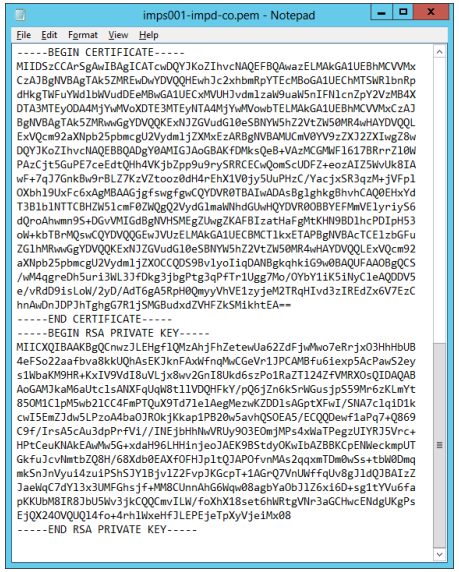
Step 11: Done with copying. Time to bounce all services; from bottom (data tier) to top (IMPS and IM)

IMPD: **dxserver stop all** then **dxserver start all** [debug process: dxserver –d start DSA_NAME_HERE]
IMCCS: **net stop im_ccs** then **net start im_ccs** [or use MS Window NT Services, services.msc] [Debug via Win Registry entry]
IMPS: **net stop im_ps** then **net start im_ps** [or use MS Windows NT Services, services.msc] [Debug via Win Registry entry]

Step 12: Validation; use Jxplorer (or openssl) to connect to all services and validate they return a full certificate.
IMPD: TCP 20391 [Newer System will also have TCP 20394, 20396, 20398, 20404] [openssl s_client –connect HOSTNAME:20391 –showcerts]
IMCCS: TCP 20403 [openssl s_client –connect HOSTNAME:20403 –showcerts]
IMPS: TCP 20390 [openssl s_client –connect HOSTNAME:20390 –showcerts]

Start the IMPS Manager GUI (IMPM) and connect to IMPS Services.





Supporting Notes

IMPS Cert Management Folder

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt\readme.txt

Identity Manager Provisioning Server provides a simple, and limited, certificate management mechanism, which allows security administrators to generate self-signed root CA certificate, client, and server certificates. The self-signed root CA certificate can then be used to sign client and server certificates.

Please note that the root CA private key is deleted at each run.

The CertMgmt directory, and its sub-directories, should be installed under ~Identity Manager\Provisioning Server\data\tls. This is because the scripts for certificate management use path relative to ~Identity Manager\Provisioning Server\bin to locate the SSL-related binaries and DLLs.

The **imps_certgen.bat** utility is used to generate Identity Manager Provisioning Server certificates.

enable_fips_mode.bat - enables FIPS 140-2 mode
disable_fips_mode.bat - disables FIPS 140-2 mode

imps_certgen.bat -> The script generates a self-signed root CA certificate, server certificate & key, and client certificate & key.

The configuration of the certificate management infrastructure is in etassl.conf.

The utility generates the following certificates at each run:
~certmgmt\data\tls\et2_cacert.pem -> Self-signed root CA certificate
~certmgmt\data\tls\server\eta2_servercert.pem -> provisioning server certificate
~certmgmt\data\tls\server\eta2_serverkey.pem -> provisioning server private key
~certmgmt\data\tls\client\eta2_clientcert.pem -> provisioning client certificate
~certmgmt\data\tls\client\eta2_clientkey.pem -> provisioning client private key

COPY FROM HERE

To deploy the new certificates on a Provisioning Server installation, replace the following installed certificates and keys by those generated above:
~Identity Manager\Provisioning Server\data\tls\et2_cacert.pem
~Identity Manager\Provisioning Server\data\tls\server\eta2_servercert.pem
~Identity Manager\Provisioning Server\data\tls\server\eta2_serverkey.pem
~Identity Manager\Provisioning Server\data\tls\client\eta2_clientcert.pem
~Identity Manager\Provisioning Server\data\tls\client\eta2_clientkey.pem

COPY TO HERE

To deploy the new certificates on a Provisioning Manager installation, replace the following installed certificates and keys by those generated above:
~Identity Manager\Provisioning Manager\data\tls\et2_cacert.pem
~Identity Manager\Provisioning Manager\data\tls\client\eta2_clientcert.pem
~Identity Manager\Provisioning Manager\data\tls\client\eta2_clientkey.pem

COPY TO HERE

To deploy the new certificates on a Provisioning Directory (data & router) installation, replace the following installed certificates and keys by those generated above:

COPY TO HERE

copy **et2_cacert.pem** to ~DXHOME\dxserver\config\ssld**impd_trusted.pem**
join **eta2_servercert.pem** AND **eta2_serverkey.pem** to new file IMPD_DSA.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-main.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-co.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-inc.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-notify.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-imps-router.pem

Note: If older system with etrustadmin.pem, etc.; replace those files with IMPD_DSA.pem AND et2_cacert.pem to etrustadmin_trusted.pem

PROCESS TO SYNC TLS CERTS FOR IMPS(&CCS), IMPM, IMPD

Impd_trusted.pem PUBLIC KEY IS THE SAME as IMPS et2_cacert.pem

imps001-impd-co (inc,main,notify,router) PUBLIC KEY IS THE SAME as IMPS eta2_servercert.pem
imps001-impd-co (inc,main,notify,router) RSA PRIVATE KEY IS THE SAME as IMPS eta2_serverkey.pem

Replace default SHA-1 with SHA-2 Certs

BOOKSHELF NOTES

Certificates	Install Location	Description
Provisioning Server Certificate	[Provisioning Server install dir]/data/tls/server/eta2_servercert.pem [Provisioning Server install dir]/data/tls/server/eta2_serverkey.pem *cs_install*/ccs/data/tls/server/eta2_servercert.pem [If NOT on IMPS Server] *cs_install*/ccs/data/tls/server/eta2_serverkey.pem [If NOT on IMPS Server] *cs_install*/jcs/conf/eta2_server.p12	Used by the Provisioning Server in .pem format and by [assign the value for iamcs in your book] in .p12 format (including signed cert, private key and root CA cert). **Note**: Import the eta2_server.p12 into *cs_install*/jcs/conf/ssl.keystore under the alias eta2_server and remove the existing entry. The ssl.keystore password is the password of the connector server that is supplied during the install.
Provisioning Client Certificate	[Provisioning Server install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Server install dir]/data/tls/client/eta2_clientkey.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientcert.pem [Provisioning Manager install dir]/data/tls/client/eta2_clientkey.pem *cs_install*/ccs/data/tls/ client/eta2_clientcert.pem [If NOT on IMPS Server] *cs_install*/ccs/data/tls/ client/eta2_clientkey.pem [If NOT on IMPS Server] *cs_install*/jcs/conf/eta2_client.p12	Used by the Provisioning Server in .pem format and by [assign the value for iamcs in your book] in .p12 format (including signed cert, private key and root CA cert).
Provisioning Directory Trusted Certificate	*cadir_install*/config/ssld/impd_trusted.pem	Used by CA Directory in .pem format. It must contain certificate content in the following structure: -----BEGIN CERTIFICATE----- Cert contents -----END CERTIFICATE-----
Provisioning Directory Personality Certificate	*cadir_install*/config/ssld/personalities/impd-co.pem *cadir_install*/config/ssld/personalities/impd-inc.pem *cadir_install*/config/ssld/personalities/impd-main.pem *cadir_install*/config/ssld/personalities/impd-notify.pem *cadir_install*/config/ssld/personalities/impd-router.pem	Used by CA Directory in .pem format.
Root CA Certificate	[Provisioning Server install dir]/data/tls/et2_cacert.pem [Provisioning Manager install dir]/data/tls/et2_cacert.pem *cs_install*/ccs/data/tls/ et2_cacert.pem [If NOT on IMPS Server] *conxp_install*/lib/jiam.jar [Application Server install dir]/iam_im.ear/library/jiam.jar	Certificate is Imported into Connector Xpress keystore located at [Connector Xpress install dir]/conf/ssl.keystore. The certificate must also be imported into the jiam.jar keystore. To import, extract the jar, import the certificate into admincacerts.jks and then repackage the jar contents. The keystore password of admincacerts.jks is "changeit". Verify that all copies of jiam.jar are replaced.

https://wiki.ca.com/cim/12-6-7/EN/configuring/ca-sso-integration/replace-native-certificates-with-sha-2-signed-ssl-certificates

CA Directory Defaults

impd\config\ssld

impd\config\ssld\personalities

dxldap.conf

TLS_CACERT C:\Program Files\CA\Directory\dxserver/config/ssld/trusted.pem

default.dxc

```
# CA Directory - DXserver/config/ssld
# This is a read-only default configuration file. If you need to make changes,
# copy this file and reference the new file from servers/<dsa>.dxi

# default CA Directory ssl configuration
# - 'dxcertgen certs' can be used to create a basic set of certificates

set ssl = {
  # folder containing DSA personality certs
  cert-dir = "config/ssld/personalities"

  # trusted root CA that signed DSA certificates
  ca-file = "config/ssld/trusted.pem"

};
```

dxcertgen certs {default.dxc}

trusted.pem {No contents; default}

CA Directory - IMPD

impd\config\ssld

impd\config\ssld\personalities

impd.dxc

```
set ssl = {
   cert-dir = "C:\Program Files\CA\Directory\dxserver\config\ssld\personalities"
   ca-file = "C:\Program Files\CA\Directory\dxserver\config\ssld\impd_trusted.pem"
   fips = false
};
```

Impd_trusted.dxc

-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----

dxcertgen -d 365 -i "dc=etadb" certs"

Will create a new entry in trusted.pem; copy / append to impd_trusted.pem.
Validate personalities were created based on DSA names.

Ref:

http://www.ca.com/us/support/ca-support-online/product-content/knowledgebase-articles/tec429160.aspx

CA Directory – IMPD – DXCERTGEN REPORT

impd\config\ssld

dxcertgen repport

impd\config\ssld\personalities

```
C:\Program Files\CA\Directory\dxserver\config\ssld>dxcertgen report
Reporting on certificates...
TRUSTED ROOT CERTIFICATES

PERSONALITY CERTIFICATES
- dxadmin.pem -
certificate : 1
version     : 1
serialNum   : 1
issuer      : /C=AU/O=DXadmin/CN=Certificate Authority
notBefore   : Feb 20 19:18:00 2012 GMT
notAfter    : Feb 20 19:18:00 2027 GMT
subject     : /C=AU/O=CA/CN=DXadmin
status      : valid

- imps001-impd-co.pem -
certificate : 1
version     : 3
serialNum   : 311
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:26:00 2007 GMT
notAfter    : Nov 25 02:26:00 2017 GMT
subject     : /C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
status      : valid

- imps001-impd-inc.pem -
certificate : 1
version     : 3
serialNum   : 311
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:26:00 2007 GMT
notAfter    : Nov 25 02:26:00 2017 GMT
subject     : /C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
status      : valid
```

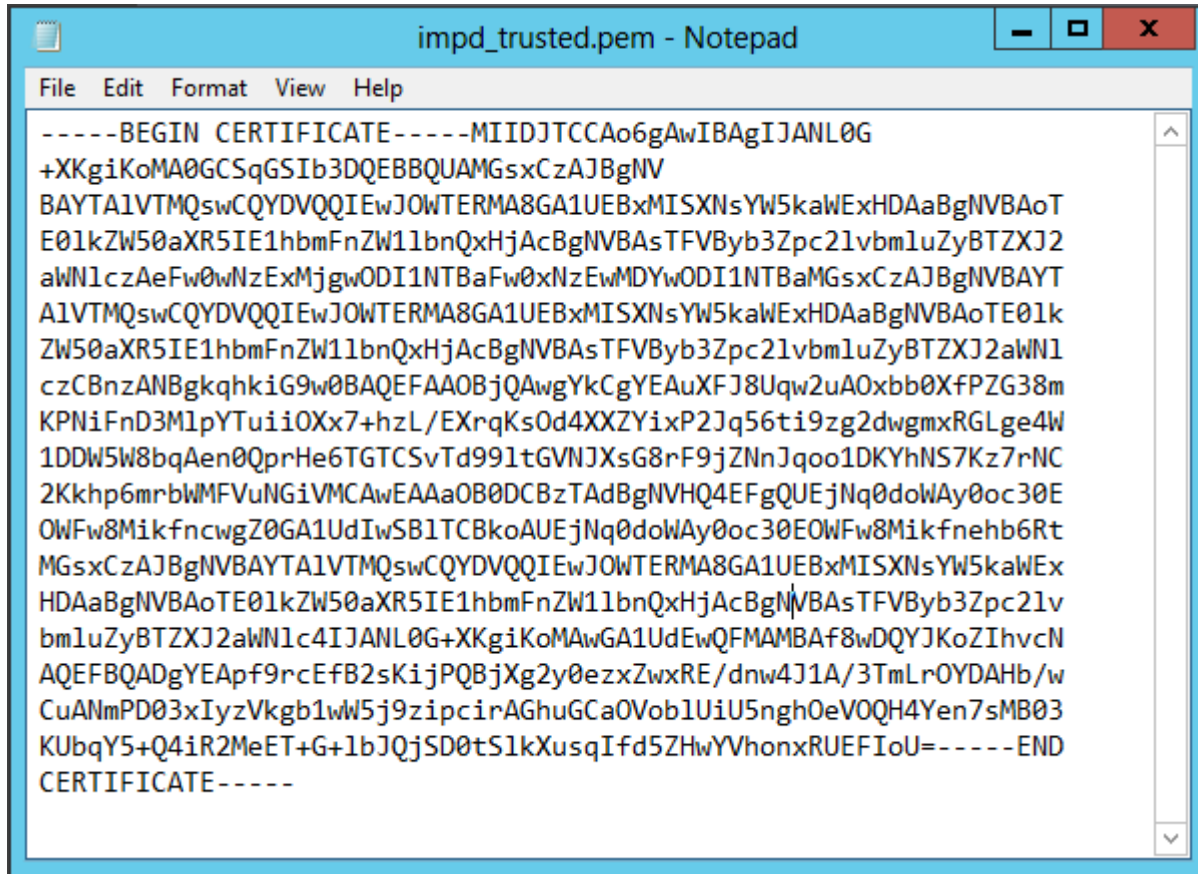
```
- imps001-impd-main.pem -
certificate : 1
version     : 3
serialNum   : 311
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:26:00 2007 GMT
notAfter    : Nov 25 02:26:00 2017 GMT
subject     : /C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
status      : valid

- imps001-impd-notify.pem -
certificate : 1
version     : 3
serialNum   : 311
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:26:00 2007 GMT
notAfter    : Nov 25 02:26:00 2017 GMT
subject     : /C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
status      : valid

- imps001-imps-router.pem -
certificate : 1
version     : 3
serialNum   : 311
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:26:00 2007 GMT
notAfter    : Nov 25 02:26:00 2017 GMT
subject     : /C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
status      : valid
```

IMPD CA Cert

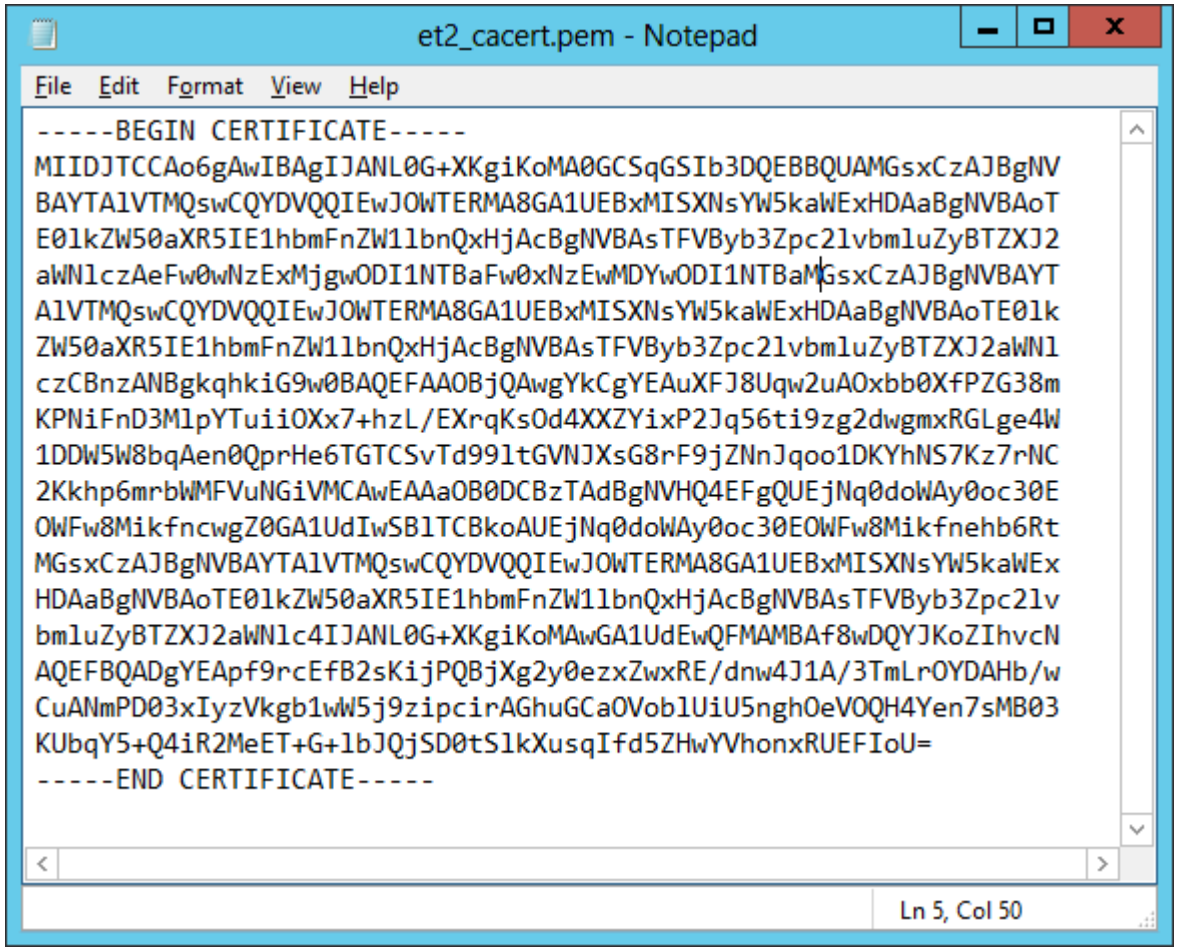
C:\Program Files\CA\Directory\dxserver\config\ssld\impd_trusted.pem



SAME but format is skewed on 1st file; seemed to have no impact

IMPS CA Cert

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\et2_cacert.pem



IMPD CA Cert

C:\Program Files\CA\Directory\dxserver\config\ssld\impd_trusted.pem

```
TRUSTED ROOT CERTIFICATES
- trusted.pem -
certificate : 1
version     : 3
serialNum   : 4294967295
issuer      : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
notBefore   : Nov 28 02:25:00 2007 GMT
notAfter    : Oct 06 02:25:00 2017 GMT
subject     : /C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
status      : valid
```

```
-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----
```

1. copy impd_trusted.pem to trusted.pem
2. dxcertgen listca

IMPS CA Cert

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\et2_cacert.pem

TCP 20390 {CA Public Key}

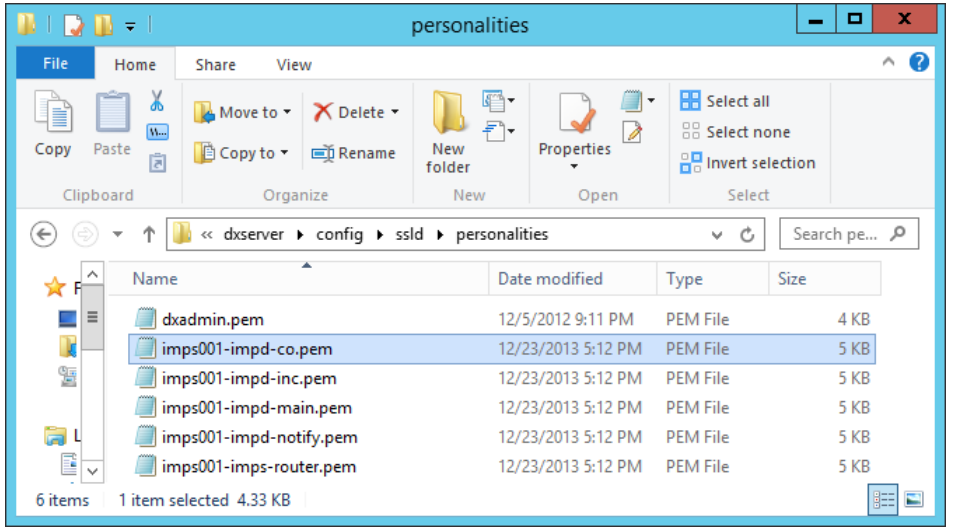
```
-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----
```

IMPD DSA Certs

Impd_trusted.pem PUBLIC KEY IS THE SAME as IMPS et2_cacert.pem

imps001-impd-co (inc,main,notify,router) PUBLIC KEY IS THE SAME as IMPS eta2_servercert.pem
imps001-impd-co (inc,main,notify,router) RSA PRIVATE KEY IS THE SAME as IMPS eta2_serverkey.pem

C:\Program Files\CA\Directory\dxserver\config\ssld\personalities\imps001-impd-co.pem




```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 311 (0x137)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=NY, L=Islandia, O=Identity Management, OU=Provisioning Services
    Validity
      Not Before: Nov 28 08:26:01 2007 GMT
      Not After : Nov 25 08:26:01 2017 GMT
    Subject: C=US, ST=NY, O=Identity Management, OU=Provisioning Services, CN=eta_server
```

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCnwzJLEHgflQMzAhjFhZetewUa62ZdFjwMwo7eRrjxO3HhHbUB
4eFSo22aafbva8kkUQhAsEKJknFAxWfnqMwCGeVr1JPCAMBfu6iexp5AcPawS2ey
s1WbaKM9HR+KxIV9VdI8uVLjx8wv2GnI8Ukd6szPo1RaZTl24ZfVMRXOsQIDAQAB
AoGAMJkaM6aUtclsANXFqUqW8tllVDQHFkY/pQ6jZn6kSrWGusjpS59Mr6zKLmYt
85OM1ClpM5wb2lCC4FmPTQuX9Td7lelAegMezwKZDDlsAGptXFwI/SNA7clqiD1k
cwI5EmZJdw5LPzoA4baOJROkjKkap1PB20w5avhQSOEA5/ECQQDewf1aPq7+Q869
C9f/IrsA5cAu3dpPrfVi//INEjbHhNwVRUy9O3EOmjMPs4xWaTPegzUIYRJ5Vrc+
HPtCeuKNAkEAwMw5G+xdaH96LHHinjeoJAEK9BStdyOKwIbAZBBKCpENWeckmpUT
GkfuJcvNmtbZQ8H/68Xdb0EAXfOFHJpltQJAPOfvnMAs2qqxmTDm0wSs+tbW0Dmq
mkSnJnVyui4zuiPShSJYlBjvlZ2FvpJKGcpT+1AGrQ7VnUWffqUv8gJldQJBAIzZ
JaeWqC7dYl3x3UMFGhsjf+MM8CUnnAhG6Wqw08agbYaObJlZ6xi6D+sg1tYVu6fa
pKKUbM8IR8JbU5Wv3jkCQQCmvILW/foXhX18set6hWRtgVNr3aGCHwcENdgUKgPs
EjQX24OVQUQl4fo+4rhlWxeHfJLEPEjeTpXyVjeiMx08
-----END RSA PRIVATE KEY-----
```

IMPS CA Server Cert

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\server\eta2_servercert.pem

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 311 (0x137)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=NY, L=Islandia, O=Identity Management, OU=Provisioning Services
    Validity
      Not Before: Nov 28 08:26:01 2007 GMT
      Not After : Nov 25 08:26:01 2017 GMT
    Subject: C=US, ST=NY, O=Identity Management, OU=Provisioning Services, CN=eta_server
```

TCP 20390 Server Public Key

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----
```

IMPS CA Server Key Cert

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\server\eta2_serverkey.pem

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCnwzJLEHgflQMzAhjFhZetewUa62ZdFjwMwo7eRrjxO3HhHbUB
4eFSo22aafbva8kkUQhAsEKJknFAxWfnqMwCGeVr1JPCAMBfu6iexp5AcPawS2ey
s1WbaKM9HR+KxIV9VdI8uVLjx8wv2GnI8Ukd6szPo1RaZTl24ZfVMRXOsQIDAQAB
AoGAMJkaM6aUtclsANXFqUqW8tllVDQHFkY/pQ6jZn6kSrWGusjpS59Mr6zKLmYt
85OM1ClpM5wb2lCC4FmPTQuX9Td7lelAegMezwKZDDlsAGptXFwI/SNA7clqiD1k
cwI5EmZJdw5LPzoA4baOJROkjKkap1PB20w5avhQSOEA5/ECQQDewf1aPq7+Q869
C9f/IrsA5cAu3dpPrfVi//INEjbHhNwVRUy9O3EOmjMPs4xWaTPegzUIYRJ5Vrc+
HPtCeuKNAkEAwMw5G+xdaH96LHHinjeoJAEK9BStdyOKwIbAZBBKCpENWeckmpUT
GkfuJcvNmtbZQ8H/68Xdb0EAXfOFHJpltQJAPOfvnMAs2qqxmTDm0wSs+tbW0Dmq
mkSnJnVyui4zuiPShSJYlBjvlZ2FvpJKGcpT+1AGrQ7VnUWffqUv8gJldQJBAIzZ
JaeWqC7dYl3x3UMFGhsjf+MM8CUnnAhG6Wqw08agbYaObJlZ6xi6D+sg1tYVu6fa
pKKUbM8IR8JbU5Wv3jkCQQCmvILW/foXhX18set6hWRtgVNr3aGCHwcENdgUKgPs
EjQX24OVQUQl4fo+4rhlWxeHfJLEPEjeTpXyVjeiMx08
-----END RSA PRIVATE KEY-----
```

IMPS CA Server Client Cert

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\client\eta2_clientcert.pem

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 312 (0x138)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=US, ST=NY, L=Islandia, O=Identity Management, OU=Provisioning Services
    Validity
      Not Before: Nov 28 08:26:10 2007 GMT
      Not After : Nov 25 08:26:10 2017 GMT
    Subject: C=US, ST=NY, O=Identity Management, OU=Provisioning Services, CN=eta_client
```

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATgwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYxMFoXDTE3MTEyNTA4MjYxMFowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9jbGllbnQwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBANx04blXS+iXptPKke+zDJcnuhGYbZHp
lW0nuGnOMX8oB0kUZTI2q6Y2rHcimhejQEoJgTCI3m++1lChQAb5Iv2pD6HImwsk
CJzHnxhcxbnCbgZs1VA1b/Gh19V+UvoKcWFxmHYneQdCUw3fXrM4rGn0ODOvtgDL
s/qzCeDMm8z1AgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFHbSePuxKyxv
qVIxWhMwLbWyI2otMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQBK
zDoNO5/+4tZisgdOYfuTcOH3mc15A9wDTNsF9eDtlkt486tNnY9akawKVA5eVP2W
+pWoFD2QkNJcC6Sbc1jAlESW948aiYHc9JQuz/I6fg/FA6AfyljcGglgrRsMEBl5
CMHQCMjGxOBI6fbfbgvpN9fMcehE5cT2IAVXP3y9vg==
-----END CERTIFICATE-----
```

IMPS CA Server Client Key Cert

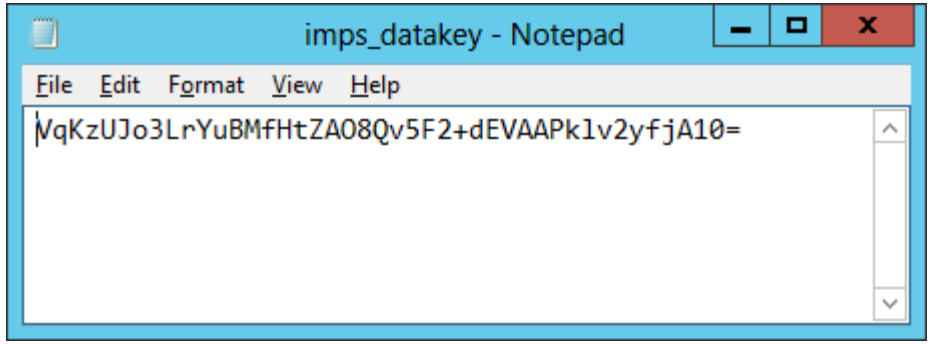
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\client\eta2_clientkey.pem

These Certs are used for the IMPS Provisioning Managers

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDcdOG5V0vol6bTypHvswyXJ7oRmG2R6ZVtJ7hpzjF/KAdJFGUy
NqumNqx3IpoXo0BKCYEwiN5vvtZQoUAG+SL9qQ+hyJsLJAicx58YXMW5wm4GbNVQ
NW/xodfVflL6CnFhcZh2J3kHQlMN316zOKxp9Dgzr7YAy7P6swngzJvM9QIDAQAB
AoGBAJl45QtaMoYhzQn0I9RzGXjBN0+4hc7mhhgPZtqBqQOUoj3F7Q0f8i8sMLRf
ala6V68zHrTjE7dHa3uGRkSUfD4/98etR4m2uVGyINs990bWvK+264F+ZaUjyqJs
h/B4HhsPh+aiTu5aozQ/K/odmotxRf5AQCTT/fhCt8kn9Z4BAkEA8hFq3iDDBcft
pUhKpMXK4jp0469ASOdCTgD7W0hFrT8zP/jIqGJc2ejAFvJz7QgymO89F/UYm1pE
5HPBkhcBpQJBAOklC5HqsEUE+teKTj3X9Ir7pVs1ouD1HbNdFEW6PGvWdICzcGP9
TMLm68cTLlGV5BETdWnAbfqO4R7kV1dBHRECQQCECRIUlSQrLBEo/VSRqb1vRllp
s7bJzTJyX8C62qH+zKFEvIuepQBmb7kPCzJGURlgJ+ZYAf1pB4TaY3VrHRdtAkAe
qzXbawDnA2Gv6syiC/9qLPIyjlqvtu7CQnNBPN9n3B0VNQWK0a5AUTogxOAp8UrA
CExArgSJmjP46Van7rPRAkEAwF3/bf43NygNu/PkUbvcYGBtVoyhUfg0GiLv74uo
tHfhNebdojOOYhGpl57xeiDwHUXDpIQ17Wbx9yvydC4IyQ==
-----END RSA PRIVATE KEY-----
```

IMPS Data Key File

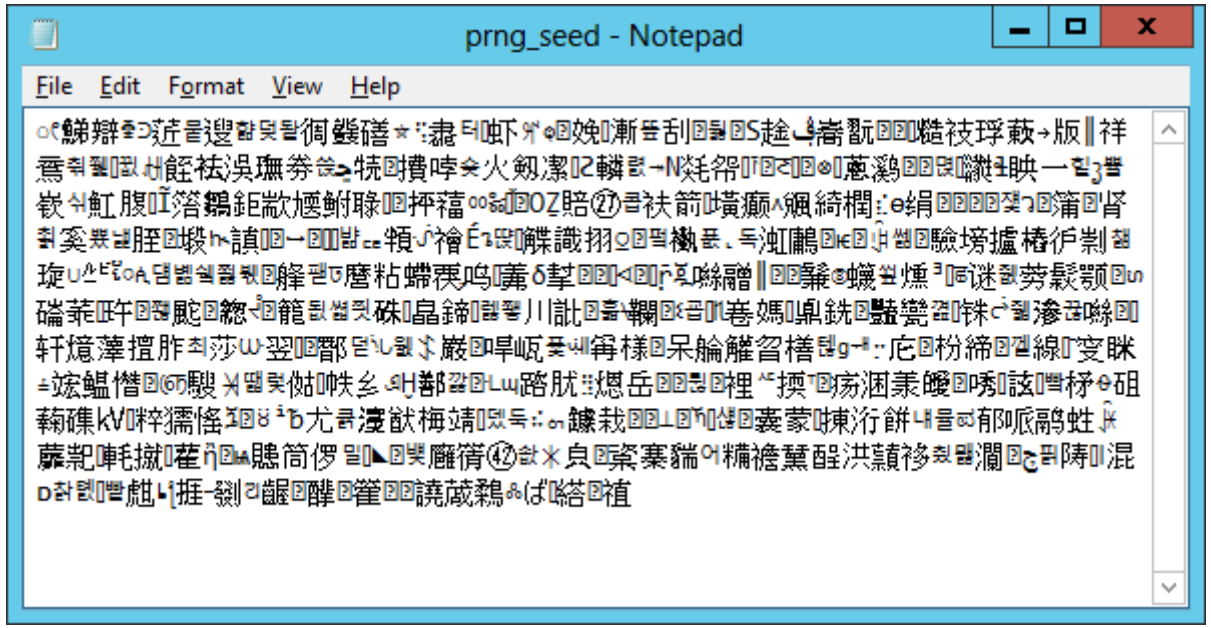
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\keymgmt\imps_datakey



VqKzUJo3LrYuBMfHtZAO8Qv5F2+dEVAAPklv2yfjA10=

IMPS PRNG SEED File

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\prng_seed



IMPS Cert Management Folder

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt\imps_certgen.bat

```
@ECHO OFF
rem This script should be run under ~Identity Manager\Provision Server\data\tls\certmgmt directory.

rem This script performs the following tasks:
rem    1. Generate a self-signed root CA cert
rem    2. Generate a server certificate and private key
rem    3. Generate a client certificate and private key
rem    4. Copy the generated root CA certificate, server certificate & key,
rem       client certificate & key to the output folder, matching IMPS deployment
rem Create location for new certs
mkdir CA\newcerts

rem    1. Generate a self-signed root CA cert
echo ------------------------------------------------------------
echo    Generate a self-signed root CA certificate for
echo        Identity Manager Provisioning Server
echo ------------------------------------------------------------
..\..\..\bin\openssl req -config .\etassl.conf -x509 -days 3600 -sha512 -newkey rsa:1024 -nodes -keyout .\CA\private\cakey.pem -out .\CA\et2_cacert.pem

rem    2   Generate a server certificate & private key
rem    2.1    Generate a server certificate request
rem    2.2    Sign the server certificate request

rem    2.1 Generate a server request
echo ------------------------------------------------------------
echo    Generate a server certificate request for
echo        Identity Manager Provisioning Server
echo ------------------------------------------------------------
..\..\..\bin\openssl req -config .\etassl.conf -sha512 -newkey rsa:1024 -nodes -keyout eta2_serverkey.pem -out .\server_req.pem

rem    2.2 Sign the server certificate request
echo ------------------------------------------------------------
echo      Sign server certificate request for
echo        Identity Manager Provisioning Server
echo ------------------------------------------------------------
..\..\..\bin\openssl ca -config .\etassl.conf -in server_req.pem -out .\eta2_servercert.pem

rem    3   Generate a server certificate & key
rem    3.1    Generate a client certificate request
rem    3.2    Sign the client certificate request

rem    3.1 Generate a client request
echo ------------------------------------------------------------
echo    Generate a client certificate request for
echo        Identity Manager Provisioning Server
echo ------------------------------------------------------------
..\..\..\bin\openssl req -config .\etassl.conf -sha512 -newkey rsa:1024 -nodes -keyout eta2_clientkey.pem -out .\client_req.pem
```

```
rem    3.2 Sign the client certificate request
echo ------------------------------------------------------------
echo      Sign client certificate request for
echo        Identity Manager Provisioning Server
echo ------------------------------------------------------------
..\..\..\bin\openssl ca -config .\etassl.conf -in client_req.pem -out .\eta2_clientcert.pem

rem Relocate the certificates for IM PS deployment
rmdir /Q /S .\data\tls\client
rmdir /Q /S .\data\tls\server
md data\tls\client
md data\tls\server

echo "moving eta2_clientkey.pem to .\data\tls\client"
copy .\eta2_clientkey.pem .\data\tls\client

echo "moving eta2_clientcert.pem to .\data\tls\client"
copy .\eta2_clientcert.pem .\data\tls\client

echo "moving eta2_serverkey.pem to .\data\tls\server"
copy .\eta2_serverkey.pem .\data\tls\server

echo "moving eta2_servercert.pem to .\data\tls\server"
copy .\eta2_servercert.pem .\data\tls\server

echo "copying et2_cacert.pem to .\data\tls"
copy .\CA\et2_cacert.pem .\data\tls

rem  DESTROY THE ROOT CA PRIVATE KEY FOR SECURITY PRUPOSE
del .\CA\private\cakey.pem

echo ------------------------------------------------------------
echo    The following certificates have been generated:
echo    .\data\tls\client\eta2_clientkey.pem
echo    .\data\tls\client\eta2_clientcert.pem
echo    .\data\tls\server\eta2_serverkey.pem
echo    .\data\tls\server\eta2_servercert.pem
echo ------------------------------------------------------------
```

IMPS Cert Management Folder

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt\etassl.conf

```
HOME                    = .
RANDFILE                = $ENV::HOME/.rnd
#oid_file               = $ENV::HOME/.oid
oid_section             = new_oids
[ new_oids ]
[ ca ]
default_ca              = CA_default
[ CA_default ]
dir                     = ./CA
certs                   = $dir/certs
crl_dir                 = $dir/crl
database                = $dir/index.txt
new_certs_dir           = $dir/newcerts
certificate             = $dir/et2_cacert.pem
serial                  = $dir/serial
crl                     = $dir/crl.pem
private_key             = $dir/private/cakey.pem
RANDFILE                = $dir/private/.rand
x509_extensions         = usr_cert
default_days            = 3650
default_crl_days        = 30
default_md              = sha512
preserve                = no
policy                  = policy_match

[ policy_match ]
countryName             = match
stateOrProvinceName= match
organizationName= match
organizationalUnitName= optional
commonName              = supplied
emailAddress            = optional
```

```
[ policy_anything ]
countryName             = optional
stateOrProvinceName= optional
localityName            = optional
organizationName= optional
organizationalUnitName= optional
commonName              = supplied
emailAddress            = optional

[ req ]
default_bits            = 1024
default_keyfile         = privkey.pem
distinguished_name= req_distinguished_name
attributes              = req_attributes
x509_extensions  = v3_ca
string_mask = nombstr

[ req_distinguished_name ]
countryName             = Country Name (2 letter code)
countryName_default             = US
countryName_min                 = 2
countryName_max                 = 2
stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default= NY
localityName            = Locality Name (eg, city)
localityName_default            = Islandia
0.organizationName              = Organization Name (eg, company)
0.organizationName_default= Identity Management
organizationalUnitName= Organizational Unit Name (eg, section)
organizationalUnitName_default= Provisioning Services
commonName              = Common Name (eg, YOUR name)
commonName_max                  = 64
emailAddress            = Email Address
emailAddress_max                = 40
```

```
[ req_attributes ]
challengePassword               = A challenge password
challengePassword_min= 4
challengePassword_max= 20
unstructuredName                = An optional company
name

[ usr_cert ]
basicConstraints=CA:FALSE
nsComment               = "OpenSSL Generated Certificate"
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always

[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = CA:true

[ crl_ext ]
authorityKeyIdentifier=keyid:always,issuer:always
```

IMPS Cert Management Folder

C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\certmgmt\readme.txt

Identity Manager Provisioning Server provides a simple, and limited, certificate management mechanism, which allows security administrators to generate self-signed root CA certificate, client, and server certificates. The self-signed root CA certificate can then be used to sign client and server certificates.

Please note that the root CA private key is deleted at each run.

The CertMgmt directory, and its sub-directories, should be installed under ~Identity Manager\Provisioning Server\data\tls. This is because the scripts for certificate management use path relative to ~Identity Manager\Provisioning Server\bin to locate the SSL-related binaries and DLLs.

The **imps_certgen.bat** utility is used to generate Identity Manager Provisioning Server certificates.

enable_fips_mode.bat - enables FIPS 140-2 mode
disable_fips_mode.bat - disables FIPS 140-2 mode

imps_certgen.bat -> The script generates a self-signed root CA certificate, server certificate & key, and client certificate & key.

The configuration of the certificate management infrastructure is in etassl.conf.

The utility generates the following certificates at each run:
~certmgmt\data\tls\et2_cacert.pem -> Self-signed root CA certificate
~certmgmt\data\tls\server\eta2_servercert.pem -> provisioning server certificate
~certmgmt\data\tls\server\eta2_serverkey.pem -> provisioning server private key
~certmgmt\data\tls\client\eta2_clientcert.pem -> provisioning client certificate
~certmgmt\data\tls\client\eta2_clientkey.pem -> provisioning client private key

COPY FROM HERE

To deploy the new certificates on a Provisioning Server installation, replace the following installed certificates and keys by those generated above:
~Identity Manager\Provisioning Server\data\tls\et2_cacert.pem
~Identity Manager\Provisioning Server\data\tls\server\eta2_servercert.pem
~Identity Manager\Provisioning Server\data\tls\server\eta2_serverkey.pem
~Identity Manager\Provisioning Server\data\tls\client\eta2_clientcert.pem
~Identity Manager\Provisioning Server\data\tls\client\eta2_clientkey.pem

COPY TO HERE

To deploy the new certificates on a Provisioning Manager installation, replace the following installed certificates and keys by those generated above:
~Identity Manager\Provisioning Manager\data\tls\et2_cacert.pem
~Identity Manager\Provisioning Manager\data\tls\client\eta2_clientcert.pem
~Identity Manager\Provisioning Manager\data\tls\client\eta2_clientkey.pem

COPY TO HERE

To deploy the new certificates on a Provisioning Directory (data & router) installation, replace the following installed certificates and keys by those generated above:

COPY TO HERE

copy **et2_cacert.pem** to ~DXHOME\dxserver\config\ssld**impd_trusted.pem**
join **eta2_servercert.pem** AND **eta2_serverkey.pem** to new file IMPD_DSA.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-main.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-co.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-inc.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-impd-notify.pem
copy **IMPD_DSA.pem** to ~DXHOME\dxserver\config\ssld\personalities\HOSTNAME-imps-router.pem

Note: If older system with etrustadmin.pem, etc.; replace those files with IMPD_DSA.pem AND et2_cacert.pem to etrustadmin_trusted.pem

Impd_trusted.pem PUBLIC KEY IS THE SAME as IMPS et2_cacert.pem

imps001-impd-co (inc,main,notify,router) PUBLIC KEY IS THE SAME as IMPS eta2_servercert.pem
imps001-impd-co (inc,main,notify,router) RSA PRIVATE KEY IS THE SAME as IMPS eta2_serverkey.pem

IMPS TCP 20390 (im_ps tls)

openssl s_client -connect imps001:20390 -showcerts

IMPS TCP 20390 SERVER PUBLIC KEY
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\server\eta2_servercert.pem
IMPS TCP 20390 CA PUBLIC KEY
C:\Program Files (x86)\CA\Identity Manager\Provisioning Server\data\tls\et2_cacert.pem

```
C:\>openssl s_client -connect imps001:20390 -showcerts
Loading 'screen' into random state - done
CONNECTED(0000012C)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----
```

```
1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----
```

```
---
Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
---
No client certificate CA names sent
---
SSL handshake has read 1972 bytes and written 511 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : AES256-GCM-SHA384
    Session-ID:
A649073CA49434274A55E4B9D18742F388FADEB6A80C669E7ECA9DE42C675D5
1
    Session-ID-ctx:
    Master-Key:
6482C9AFDEEE5AC1C6268D6716526D4F402A4855BFF1BB0DCC4BFEEFBF3859A
0731328FEFE1B9647B80B7E6525096511
```

```
Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 63 61 5e b5 62 9d 99 42-95 8e c1 34 f9 54 3e 12   ca^.b..B...4.T>.
    0010 - b0 a5 cd 53 95 7d 9a 39-a6 81 02 64 97 1b 61 33   ...S.}.9...d..a3
    0020 - a0 a2 b3 f7 74 61 cd f9-98 bd 14 20 35 cb 2f e6   ....ta..... 5./.
    0030 - 3f 8b b2 71 af d6 9e 7c-67 79 f3 83 8e 19 7b c4   ?..q...|gy....{.
    0040 - c3 a3 76 11 58 ad 27 6b-80 fb 08 59 07 6a e7 c9   ..v.X.'k...Y.j..
    0050 - 25 4f 18 4b d8 e2 2e 54-e1 95 17 e2 e7 ee 4a 92   %O.K...T......J.
    0060 - 5c c3 80 a0 95 4b c6 31-d4 24 45 80 b7 a6 59 cc   \....K.1.$E...Y.
    0070 - 2d 31 ae 3f 54 e1 06 11-43 39 49 e6 71 f6 f8 ed   -1.?T...C9I.q...
    0080 - f8 17 17 33 de e8 7e 90-73 fa 06 89 05 92 4b 24   ...3..~.s.....K$
    0090 - d8 00 f3 4a b4 34 04 92-1d 4a bf 00 9e fa 20 5e   ...J.4...J.... ^

    Start Time: 1447369557
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
```

IMPS TCP 20391 (Router DSA)

openssl s_client -connect imps001:20391 -showcerts

```
C:\>openssl s_client -connect imps001:20391 -showcerts
Loading 'screen' into random state - done
CONNECTED(0000013C)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----
```

```
1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
  i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----
```

```
---
Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
---
No client certificate CA names sent
---
SSL handshake has read 2388 bytes and written 531 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID:
B324607D24F8BB4CCB9E1C27FA132FCF916F816FDFE3B656A58D41126867CABC
    Session-ID-ctx:
    Master-Key:
CA1DB99BAD2623DEAF590340943AB723C33A1FF4A2EA2E37F4400DBF873444B
776CA0BD2B0B7C074D81A6BD8652885C6
```

```
Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket:
    0000 - 36 c6 5c 2e d6 d9 ef 55-f0 48 db c9 f9 25 29 3d   6.\....U.H...%)=
    0010 - e5 dc 9e 0f 68 c7 3f a2-98 02 6f 8e 11 76 c0 89   ....h.?...o..v..
    0020 - 5a 1e 9a 7c 8b 53 04 0d-74 9a 4f 73 59 1b 78 33   Z..|.S..t.OsY.x3
    0030 - 2f 53 cd 73 21 4c 04 80-7f 41 50 94 5a b0 fe 1b   /S.s!L...AP.Z...
    0040 - 65 9c 20 e8 83 12 cd 89-e8 bc f1 80 39 a3 ec ee   e. .........9...
    0050 - c2 cd f4 b9 85 ca 29 f3-54 6c f8 9f 1d 20 ea c0   ......).Tl... ..
    0060 - 2c 5a d4 8f e4 7a cc c0-65 e9 ce 6a 15 b7 5a c9   ,Z...z..e..j..Z.
    0070 - c9 d4 59 60 ec d5 ff a5-32 11 fd 81 24 99 79 e5   ..Y`....2...$.y.
    0080 - c2 a9 3f f5 48 e2 f4 1e-d6 63 23 64 f2 08 92 84   ..?.H....c#d....
    0090 - b2 f5 50 8a 03 59 64 ee-45 95 c5 f5 82 fd 77 2d   ..P..Yd.E.....w-

    Start Time: 1447370267
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
```

IMPD TCP 20391 SERVER PUBLIC KEY C:\Program Files\CA\Directory\dxserver\config\ssld\personalities\imps001-impd-router.pem (main,inc,notify,co)
IMPD TCP 20391 CA PUBLIC KEY C:\Program Files\CA\Directory\dxserver\config\ssld\impd_trusted.pem

IMPD TCP 20394 (Data DSA)

openssl s_client -connect imps001:20394 -showcerts

C:\>**openssl s_client -connect imps001:20394 -showcerts**
Loading 'screen' into random state - done
CONNECTED(0000013C)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0

Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----

1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
  i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----

Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

---
No client certificate CA names sent

SSL handshake has read 2388 bytes and written 531 bytes

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : DHE-RSA-AES256-SHA
    Session-ID:
668D2312C57FF7F0FA47F3E6E49FDB03A96BF19922829EF38D6A519C97F501B0
    Session-ID-ctx:
    Master-Key:
423F39B4623A19328CA1FE8B91593476799F60F43ECCCB2BDF70BB385078270C6
8B939112B59325D8B7353789CA53C2F

Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket:
    0000 - a6 1b c7 f5 b5 dc be 7a-da a7 54 fa 45 ad a2 7a   ....z..T.E..z
    0010 - 92 3f 07 a3 fb 1f 87 df-29 04 71 4f b8 5d 5b 25   .?......).qO.][%
    0020 - 46 76 8e 71 0e 69 ff d0-32 df d1 00 e2 c9 a9 c0   Fv.q.i..2.......
    0030 - c9 4b ed 2a ae d3 55 ca-30 15 66 ed 70 5f 9a 3c   .K.*..U.0.f.p_.<
    0040 - 84 1c 8b bf 53 36 a0 e6-68 36 53 cd 8d a0 2e f0   ....S6..h6S.....
    0050 - 95 13 73 88 01 31 c4 7d-40 b8 1a 06 7c 88 85 31   ..s..1.}@...|..1
    0060 - 8a 96 94 80 77 5e 5f e3-9d 56 17 5a b6 5f 91 3a   ....w^_..V.Z._.:
    0070 - f3 34 e8 20 a6 98 a0 23-7c 59 54 ac 17 6d 3d b3   .4. ...#|YT..m=.
    0080 - c0 da bc 44 b5 9b 1c c0-ee f8 ab ef ea d1 2b 8c   ...D..........+.
    0090 - 39 64 9a 2f e6 6e f9 3c-56 2e 9d 30 bb 1a 99 40   9d./.n.<V..0...@

    Start Time: 1447370801
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)

IMPD TCP 20391 SERVER PUBLIC KEY
C:\Program Files\CA\Directory\dxserver\config\ssld\personalities\imps001-impd-main.pem (router,inc,notify,co)
IMPD TCP 20391 CA PUBLIC KEY
C:\Program Files\CA\Directory\dxserver\config\ssld\impd_trusted.pem

IAMCS TCP 20443 (Web UI)

openssl s_client -connect imps001:20443 -showcerts

keytool -import -trustcacerts -keystore "conxp-home/conf/ssl.keystore" -file trusted-certificate.pem

C:\>**openssl s_client -connect imps001:20443 -showcerts**
Loading 'screen' into random state - done
CONNECTED(00000144)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0
1200:error:1408D13A:SSL routines:SSL3_GET_KEY_EXCHANGE:unable to find ecdh parameters:.\ssl\s3_clnt.c:1634:

Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----

1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
  i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----

Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

---
No client certificate CA names sent

SSL handshake has read 2044 bytes and written 7 bytes

New, (NONE), Cipher is (NONE)
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE

SSL-Session:
  Protocol : TLSv1.2
  Cipher   : 0000
  Session-ID:
56452229B2FE937F28734EB22B308FCD310D98B2927B80EBDDC3305
8B3DB2684
  Session-ID-ctx:
  Master-Key:
  Key-Arg   : None
  PSK identity: None
  PSK identity hint: None
  SRP username: None
  Start Time: 1447371305
  Timeout   : 300 (sec)
  Verify return code: 19 (self signed certificate in certificate chain)
---

https://wiki.ca.com/display/IMGC10/Import+the+CA+LDAP+Server+Certificate+into+the+CA+IAM+CS+Keystore

IAMCS TCP 20411 (im_jcs tls)

openssl s_client -connect imps001:20411 -showcerts

```
C:\>openssl s_client -connect imps001:20411 -showcerts
Loading 'screen' into random state - done
CONNECTED(00000094)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----
```

```
1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
  i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----
```

```
---
Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
```

```
---
No client certificate CA names sent
---
SSL handshake has read 2344 bytes and written 519 bytes
---
New, TLSv1/SSLv3, Cipher is EDH-RSA-DES-CBC3-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
```

```
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : EDH-RSA-DES-CBC3-SHA
    Session-ID:
564524961E871E8B7B5046C42A775C59F18849A6381FE8B0F7896670ACC103B7
    Session-ID-ctx:
    Master-Key:
52890B5C403B5FC509DBD12B3CD840005D1602F69E1BCC5E7880ECB5214781F
553A9BEE6BDD7157B7A5FE49564AE74B1
    Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1447371926
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
```

IM CCS TCP 20403 (im_ccs tls)

openssl s_client -connect imps001:20403 -showcerts

C:\>**openssl s_client -connect imps001:20403 -showcerts**
Loading 'screen' into random state - done
CONNECTED(00000130)
depth=1 C = US, ST = NY, L = Islandia, O = Identity Management, OU = Provisioning Services
verify error:num=19:self signed certificate in certificate chain
verify return:0

Certificate chain
 0 s:/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
   i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDSzCCArSgAwIBAgICATcwDQYJKoZIhvcNAQEFBQAwazELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAk5ZMREwDwYDVQQHEwhJc2xhbmRpYTEcMBoGA1UEChMTSWRlbnRp
dHkgTWFuYWdlbWVudDEeMBwGA1UECxMVUHJvdmlzaW9uaW5nIFNlcnZpY2VzMB4X
DTA3MTEyODA4MjYwMVoXDTE3MTEyNTA4MjYwMVowbTELMAkGA1UEBhMCVVMxCzAJ
BgNVBAgTAk5ZMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQL
ExVQcm92aXNpb25pbmcgU2VydmljZXMxEzARBgNVBAMUCmV0YV9zZXJ2ZXIwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKfDMksQeB+VAzMCGMWFl617BRrrZl0W
PAzCjt5GuPE7ceEdtQHh4VKjbZpp9u9rySRRCECwQomScUDFZ+eozAIZ5WvUk8IA
wF+7qJ7GnkBw9rBLZ7KzVZtooz0dH4rEhX1V0jy5UuPHzC/YacjxSR3qzM+jVFpl
OXbhl9UxFc6xAgMBAAGjgfswgfgwCQYDVR0TBAIwADAsBglghkgBhvhCAQ0EHxYd
T3BlblNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNhdGUwHQYDVR0OBBYEFMmVElyriyS6
dQroAhwmn9S+DGvVMIGdBgNVHSMEgZUwgZKAFBIzatHaFgMtKHN9BDlhcPDIpH53
oW+kbTBrMQswCQYDVQQGEwJVUzELMAkGA1UECBMCTlkxETAPBgNVBAcTCElzbGFu
ZGlhMRwwGgYDVQQKExNJZGVudGl0eSBNYW5hZ2VtZW50MR4wHAYDVQQLExVQcm92
aXNpb25pbmcgU2VydmljZXOCCQDS9BvlyoIiqDANBgkqhkiG9w0BAQUFAAOBgQCS
/wM4qgreDh5uri3WL3JfDkg3jbgPtg3qPfTr1Ugg7Mo/OYbY1iK5iNyCleAQDDV5
e/vRdD9isLoW/2yD/AdT6gA5RpH0QmyyVhVE1zyjeM2TRqHIvd3zIREdZx6V7EzC
hnAwDnJDPJhTghgG7R1jSMGBudxdZVHFZkSMikhtEA==
-----END CERTIFICATE-----

1 s:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services
  i:/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

-----BEGIN CERTIFICATE-----
MIIDJTCCAo6gAwIBAgIJANL0G+XKgiKoMA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
BAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoT
E0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2
aWNlczAeFw0wNzExMjgwODI1NTBaFw0xNzEwMDYwODI1NTBaMGsxCzAJBgNVBAYT
AlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWExHDAaBgNVBAoTE0lk
ZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lvbmluZyBTZXJ2aWNl
czCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuXFJ8Uqw2uAOxbb0XfPZG38m
KPNiFnD3MlpYTuiiOXx7+hzL/EXrqKsOd4XXZYixP2Jq56ti9zg2dwgmxRGLge4W
1DDW5W8bqAen0QprHe6TGTCSvTd99ltGVNJXsG8rF9jZNnJqoo1DKYhNS7Kz7rNC
2Kkhp6mrbWMFVuNGiVMCAwEAAaOB0DCBzTAdBgNVHQ4EFgQUEjNq0doWAy0oc30E
OWFw8MikfncwgZ0GA1UdIwSBlTCBkoAUEjNq0doWAy0oc30EOWFw8Mikfnehb6Rt
MGsxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJOWTERMA8GA1UEBxMISXNsYW5kaWEx
HDAaBgNVBAoTE0lkZW50aXR5IE1hbmFnZW1lbnQxHjAcBgNVBAsTFVByb3Zpc2lv
bmluZyBTZXJ2aWNlc4IJANL0G+XKgiKoMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcN
AQEFBQADgYEApf9rcEfB2sKijPQBjXg2y0ezxZwxRE/dnw4J1A/3TmLrOYDAHb/w
CuANmPD03xIyzVkgb1wW5j9zipcirAGhuGCaOVoblUiU5nghOeVOQH4Yen7sMB03
KUbqY5+Q4iR2MeET+G+lbJQjSD0tSlkXusqIfd5ZHwYVhonxRUEFIoU=
-----END CERTIFICATE-----

Server certificate
subject=/C=US/ST=NY/O=Identity Management/OU=Provisioning Services/CN=eta_server
issuer=/C=US/ST=NY/L=Islandia/O=Identity Management/OU=Provisioning Services

---
No client certificate CA names sent

SSL handshake has read 1972 bytes and written 511 bytes

New, TLSv1/SSLv3, Cipher is AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : AES256-GCM-SHA384
    Session-ID:
981EE967F7341319FA8F76F964146BC4D55C87B108F78E88274C9AEB832A901A
    Session-ID-ctx:
    Master-Key:
699406E9495094A13CB3794DDF13A63582A72C8F31DC736B6BDBE2D2CA37B2F
22454EBFA60CCE9D116493ED992CEF594

Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - d2 ec 5f 29 87 15 f8 d4-77 9b d9 7c ca da 37 93   .._)....w..|..7.
    0010 - e4 12 b1 9a 65 81 a9 07-ef bc 74 45 ec ab a7 19   ....e.....tE....
    0020 - b8 a3 d7 fa 52 f1 ee 6f-7f 5e 74 01 a2 0c f7 aa   ....R..o.^t.....
    0030 - bf 1e 39 b9 d1 4e 71 4e-85 6d 01 6a af f4 09 15   ..9..NqN.m.j....
    0040 - ca f3 cf 46 ec ac 03 c6-e9 f8 58 41 fa 0f 89 db   ...F......XA....
    0050 - 79 37 6f 2a 43 63 0c 39-86 11 74 e8 a0 9f 20 c7   y7o*Cc.9..t... .
    0060 - 82 de 8c 79 cd a8 76 e4-78 be 51 fd b9 ef 7b 08   ...y..v.x.Q...{.
    0070 - 3b 8e d5 5d 34 37 c7 76-06 d5 10 ce 03 34 4c 93   ;..]47.v.....4L.
    0080 - 30 47 0b 73 53 78 30 cf-87 60 1d 37 5d fb 19 74   0G.sSx0..`.7]..t
    0090 - 2b 34 3b 81 54 c9 9d 8a-7a 57 d4 65 02 92 0b 39   +4;.T...zW.e...9

    Start Time: 1447372167
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)

IMPS TCP 20389 (im_ps no tls)

openssl s_client -connect imps001:20389 -showcerts

```
C:\>openssl s_client -connect imps001:20389 -showcerts
Loading 'screen' into random state - done
CONNECTED(00000144)
write:errno=10054
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 0 bytes and written 321 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
---
```

SHOWN ONLY AS COMPARISION FOR NON-TLS SERVICES

IMPS TCP 4105 (cam)

openssl s_client -connect imps001:4105 -showcerts

```
C:\>openssl s_client -connect imps001:4105 -showcerts
Loading 'screen' into random state - done
CONNECTED(000000E0)
write:errno=10054
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 4 bytes and written 321 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
---
```

IAMCS TCP 20410
IM CCS TCP 20402

DXADMIND TCP 2123 (tls)

openssl s_client -connect imps001:20403 -showcerts

DXADMIND TCP 2123 SERVER PUBLIC KEY
C:\Program Files\CA\Directory\dxserver\config\ssld\personalities\dxadmin.pem
DXADMIND TCP 2121 CA PUBLIC KEY
C:\Program Files\CA\Directory\dxserver\config\ssld\dxadminCA.pem

C:**openssl s_client -connect imps001:2123 -showcerts**
Loading 'screen' into random state - done
CONNECTED(00000138)
depth=1 C = AU, O = DXadmin, CN = Certificate Authority
verify error:num=19:self signed certificate in certificate chain
verify return:0

Certificate chain
 0 s:/C=AU/O=CA/CN=DXadmin
   i:/C=AU/O=DXadmin/CN=Certificate Authority

-----BEGIN CERTIFICATE-----
MIIB9TCCAV4CCQDHXIUlShSw5TANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJB
VTEQMA4GA1UEChMHRFhhZG1pbjEeMBwGA1UEAxMVQ2VydGlmaWNhdGUgQXV0aG9y
aXR5MB4XDTEyMDIyMTAxMTgyMloXDTI3MDIyMTAxMTgyMlowPzELMAkGA1UEBhMC
QVUxEDAOBgNVBAoTB0RYYWRtaW4xHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1dGhv
cml0eTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1pakMOJ5qnkTTLcOEvjo
viDE74lDJunxpAFSiOrP4vtPUKOiRweJ2TBUZERSjl4bzbngjHwOp1JXbBkCm926
mzDp5KoWrH27xJJSvJgDud1kXOLtfAAlrar+orc2o5biE02hvsJgfQQc8wwzRK1J
lnFT2m09jaweYfb/tSYQ2K8CAwEAATANBgkqhkiG9w0BAQUFAAOBgQCpVqyFn6ba
f9ZbPmcGDnnioAXwLCjYN4f9vsJ3Bn76QRPX22c7RddiBrzg/NL8ii4Eeu3jVvmw
H3LmJHdWgPAznKzz1WwRtf8+uYv74LF29xRaXjINniYO9Ou+rVE0q9yqBP37DapA
yGCPCerasOWwyjjQNPpJ9viXWklB6dzwHQ==
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIB2jCCAUMCAQEwDQYJKoZIhvcNAQEEBQAwPzELMAkGA1UEBhMCQVUxEDAOBgNV
BAoTB0RYYWRtaW4xHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0x
MjAyMjEwMTE4MjJaFw0yNzAyMjEwMTE4MjJaMCwxCzAJBgNVBAYTAkFVMQswCQYD
VQQKEwJDQTEQMA4GA1UEAxMHRFhhZG1pbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEA9OfkRSFSmOvmt6mj1WMhxhQqzajqf2ypeaQYD4WH6QoSyGp0QsoDL0hW
1TWgPDztTmWXnbj7lf2sF7N1B4KIUkRsTXgKIGZI7denDVNXcxonzZ57B9qX695o
b8htc23TnexOyX07KCcq6V4FLVkihmjiJwYmt5z64pPWU6u0c+0CAwEAATANBgkq
hkiG9w0BAQQFAAOBgQDKrZQoQg9aO08iJjVqq+5hyP+lT9oa5RMm6v6ZR9b0hmNO
rpqhNmX75JnrNT+Ej7TwbLqbvj9R1T4RGx4vf65SRKUXFLlN/X56jsIILHVmwH56
q5DUX/r3hARTZMvap9CVPQa191/PnbZMulV5AZs2/5VSNg9WyiZH3gI/mZGfrg==
-----END CERTIFICATE-----

Server certificate
subject=/C=AU/O=CA/CN=DXadmin
issuer=/C=AU/O=DXadmin/CN=Certificate Authority

1 s:/C=AU/O=DXadmin/CN=Certificate Authority
  i:/C=AU/O=DXadmin/CN=Certificate Authority

No client certificate CA names sent

SSL handshake has read 1302 bytes and written 519 bytes

New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1
    Cipher   : AES256-SHA
    Session-ID:
2BC60D99C48C38BEFE8E3DED36F44B8C9B31C2D322E74D2770A50BD1801A68D
F
    Session-ID-ctx:
    Master-Key:
971FFF34DAD5F6DF2CB884E9BD536AED32AAA4756DE4791E6BDD61596693A7D
0E51929439F0A3C90DAA9297DA1639A24

Key-Arg   : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket:
    0000 - cc 24 38 ac f4 70 4f b2-db e7 58 71 41 7c dc 51   .$8..pO...XqA|.Q
    0010 - 23 8d ed 78 d6 d9 91 c7-e5 6f 3e db 1e 22 37 f8   #..x.....o>.."7.
    0020 - e7 ee 0d 7c d3 10 a9 cb-68 39 13 e8 76 b5 15 a5   ...|....h9..v...
    0030 - ef 8e 29 f0 c4 0a e8 10-d3 de 4f cd d0 0c f3 d2   ..).......O.....
    0040 - 56 99 6d f8 42 1d ba cf-e0 7a b2 d2 3b f5 88 9a   V.m.B....z..;...
    0050 - fe 9a 7f a9 e7 fe a7 3b-67 4c 04 0e f9 0c 42 cb   ....;gL....B.
    0060 - da f5 0f 13 f9 ab b7 c5-4b 5a 8c 57 e6 6d 95 63   ........KZ.W.m.c
    0070 - 95 00 12 60 01 76 d3 84-e6 c5 f6 e6 56 9b 9d 84   ...`.v......V...
    0080 - fe dc 11 a3 02 5d 1b 07-d4 1a aa fc b2 68 79 3f   .....].......hy?
    0090 - f7 d2 e1 cc 63 01 ce d2-28 d3 8f 3a d7 ae 4b cd   ....c...(..:..K.

    Start Time: 1447372364
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)

DXADMIND Server Cert

C:\Program Files\CA\Directory\dxserver\config\ssld\personalities\dxadmin.pem

```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=AU, O=DXadmin, CN=Certificate Authority
    Validity
      Not Before: Feb 21 01:18:22 2012 GMT
      Not After : Feb 21 01:18:22 2027 GMT
    Subject: C=AU, O=CA, CN=DXadmin
```

```
-----BEGIN CERTIFICATE-----
MIIB2jCCAUMCAQEwDQYJKoZIhvcNAQEEBQAwPzELMAkGA1UEBhMCQVUxEDAOBgNV
BAoTB0RYYWRtaW4xHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1dGhvcml0eTAeFw0x
MjAyMjEwMTE4MjJaFw0yNzAyMjEwMTE4MjJaMCwxCzAJBgNVBAYTAkFVMQswCQYD
VQQKEwJDQTEQMA4GA1UEAxMHRFhhZG1pbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEA9OfkRSFSmOvmt6mj1WMhxhQqzajqf2ypeaQYD4WH6QoSyGp0QsoDL0hW
1TWgPDztTmWXnbj7lf2sF7N1B4KIUkRsTXgKIGZI7denDVNXcxonzZ57B9qX695o
b8htc23TnexOyX07KCcq6V4FLVkihmjiJwYmt5z64pPWU6u0c+0CAwEAATANBgkq
hkiG9w0BAQQFAAOBgQDKrZQoQg9aO08iJjVqq+5hyP+lT9oa5RMm6v6ZR9b0hmNO
rpqhNmX75JnrNT+Ej7TwbLqbvj9R1T4RGx4vf65SRKUXFLlN/X56jsIILHVmwH56
q5DUX/r3hARTZMvap9CVPQa191/PnbZMulV5AZs2/5VSNg9WyiZH3gI/mZGfrg==
-----END CERTIFICATE-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQD05+RFIVKY6+a3qaPVYyHGFCrNqOp/bKl5pBgPhYfpChLIanRC
ygMvSFbVNaA8PO1OZZeduPuV/awXs3UHgohSRGxNeAogZkjt16cNU1dzGifNnnsH
2pfr3mhvyG1zbdOd7E7JfTsoJyrpXgUtWSKGaOInBia3nPrik9ZTq7Rz7QIDAQAB
AoGALBxIRRtHYTu8BoCLfbepMaAYRYqTEfhkXgBsRP9sB1FFKMvjvNPd1vpUiXpr
Le5bX690q3fR+KYEBRDRl1SvcKenf4TZ5BdzyI2WA67PoazHCc5eaKnJRLSA0U0p
7iDERV8ftn2ORLzi15RlN+TjamWqueF8hQZIkj8T/llaMhECQQD6gUZMGVf7ti6H
bXpRVK5FuFhkYD8SVEA2GzN/mgvUuXoSHplyj5ESD2JxYQ8vVyw2prrWQQtQQCOV
bqAlxCtfAkEA+kcsuhf5OkGMiOdk7PID+aLCDqNZpqZsz9OoxB1UzS/eNHjDOrak
+xdwjzGZ6QHCnrt5zWIxI+wYcN3pMUIwMwJAJRiJuXEzV0IWR9XNfEfG+uoepNaf
4G37iEek66t7PwgsbIx9erqJ6BvBHzsZTZBiKsGr/1hofXzSCCn2q0EOjwJALjVd
6K3scfkQPWabl7PHUBvgwFsgfkhT5rspeawAsDGaUQ3K3dhC9akKOyXpSL/ucugi
QO1ULVG14YDXQST7SQJBAJ/YAsYdXa7JHSpiXG3O7Xpkw4V26te82ah31nXGFRHf
AVbHNhA7nHvPVFHT9V5uGRR2Rmfzd9HceuKW2Qr+5Cw=
-----END RSA PRIVATE KEY-----
```

TCP 2123 Server Public Key

DXADMIND CA Cert

C:\Program Files\CA\Directory\dxserver\config\ssld\dxadminCA.pem

```
Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number:
      c7:5c:85:25:4a:14:b0:e5
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=AU, O=DXadmin, CN=Certificate Authority
    Validity
      Not Before: Feb 21 01:18:22 2012 GMT
      Not After : Feb 21 01:18:22 2027 GMT
    Subject: C=AU, O=DXadmin, CN=Certificate Authority
```

```
-----BEGIN CERTIFICATE-----
MIIB9TCCAV4CCQDHXIUlShSw5TANBgkqhkiG9w0BAQUFADA/MQswCQYDVQQGEwJB
VTEQMA4GA1UEChMHRFhhZG1pbjEeMBwGA1UEAxMVQ2VydGlmaWNhdGUgQXV0aG9y
aXR5MB4XDTEyMDIyMTAxMTgyMloXDTI3MDIyMTAxMTgyMlowPzELMAkGA1UEBhMC
QVUxEDAOBgNVBAoTB0RYYWRtaW4xHjAcBgNVBAMTFUNlcnRpZmljYXRlIEF1dGhv
cml0eTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA1pakMOJ5qnkTTLcOEvjo
viDE74lDJunxpAFSiOrP4vtPUKOiRweJ2TBUZERSjl4bzbngjHwOp1JXbBkCm926
mzDp5KoWrH27xJJSvJgDud1kXOLtfAAlrar+orc2o5biE02hvsJgfQQc8wwzRK1J
lnFT2m09jaweYfb/tSYQ2K8CAwEAATANBgkqhkiG9w0BAQUFAAOBgQCpVqyFn6ba
f9ZbPmcGDnnioAXwLCjYN4f9vsJ3Bn76QRPX22c7RddiBrzg/NL8ii4Eeu3jVvmw
H3LmJHdWgPAznKzz1WwRtf8+uYv74LF29xRaXjINniYO9Ou+rVE0q9yqBP37DapA
yGCPCerasOWwyjjQNPpJ9viXWklB6dzwHQ==
-----END CERTIFICATE-----
```

HOW TO UPDATE THE TLS CERTS IN PDI

aUse PDI Transformations on a Server with SSL Configured

To use PDI transformations on a CA GovernanceMinder server that is configured with SSL, use the following procedure.

Note: For more information on how to configure a CA GovernanceMinder server for SSL communication, see the *Installation Guide*.

Follow these steps:

1.Install OpenSSL.

2.Open a command prompt and run the following command: `openssl s_client -connect RCM_HOST:8443`

3.Copy all text between the following (including the begin and end lines) to a cert.txt file:`----BEGIN CERTIFICATE---- ----END CERTIFICATE----`

4.Run the following command to verify the certificate:`"%JAVA_HOME%\bin\keytool" -printcert -file cert.txt`

5.Create a rcmServer.keystore file by using the key tool, as follows:`"%JAVA_HOME%\bin\keytool" -import -file cert.txt -keystore rcmSrever.keystore -storepass password`

The file is created under the java bin directory.

6.Copy the rcmServer.keystore file to the PDI home directory.

7.Edit the PDI application files, as follows:

- Windows: Edit set-pentaho-env.bat and add the following:`set PENTAHO_DI_JAVA_OPTIONS =%PENTAHO_DI_JAVA_OPTIONS% Djavax.net.ssl.trustStore=rcmSrever.keystore -Djavax.net.ssl.keyStorePassword=password`
- Linux: Edit set-pentaho-env.sh and add the following:`PENTAHO_DI_JAVA_OPTIONS ="$ PENTAHO_DI_JAVA_OPTIONS Djavax.net.ssl.trustStore=rcmSrever.keystore -Djavax.net.ssl.keyStorePassword=password"`

8.Open the spoon.bat/sh file and add the Input step for Users to a transformation.

9.Edit the Input Users step, and click Edit the RCM Connection.

10.Verify the following:

1. The RCM connection information lists https://servername:sslPort as the connection URL.
2. The Accept any certificate check box is cleared.
3. Click Test RCM Connection.

https://support.ca.com/cadocs/0/CA%20GovernanceMinder%2012%206%201-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1957698.html

HOW TO UPDATE THE TLS CERTS IN CX

Set Up TLS/SSL for a JNDI Data Source

In Connector Xpress, you can define a JNDI data source as TLS/SSL enabled.

If a JNDI data source is TLS/SSL enabled, import the JNDI data source certificate into the Connector Xpress trusted certificate store.

Follow these steps:

1.Create a PEM file for each issuer in the target certificate's chain.

2.For each file enter the following command:`keytool -import -trustcacerts -keystore "`*`conxp-home`*`/conf/ssl.keystore" -file `*`trusted-certificate`*`.pem`

The JNDI Data Source certificate is imported into the ssl.keystore

Repeat this command for each PEM file.

3.Restart Connector Xpress.

4.Test the TLS/SSL connection in Connector Xpress.

https://support.ca.com/cadocs/0/CA%20GovernanceMinder%2012%206%201-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?2016283.html?zoom_highlight=tls

https://support.ca.com/cadocs/0/CA%20GovernanceMinder%2012%206%201-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1957698.html

HOW TO UPDATE FIPS

How To Enable FIPS 140-2 Encryption

Federal Information Processing Standards (FIPS) 140-2 is a US federal standard that dictates the security requirements for cryptographic modules that are utilized within a security system protecting sensitive information in computer systems.

The product makes limited use of encryption, primarily to protect passwords and other information that is used to access other applications, databases, or operating environments.

To enable FIPS 140-2 compliant encryption in CA GovernanceMinder, do the following:

•Implement Transport Layer Security (TLS/SSL) protection at the application server level.

•Provide an acceptable level of key (passphrase) security.

•Download and install Java security components.

•Configure the product to use FIPS-certified encryption algorithms. CA uses the RSA Crypto-J library for FIPS-compliant encryption.

Important! If FIPS-compliant encryption is adopted *after* the product begins to function, inconsistencies can result. Previously encrypted data can be rendered inaccessible, and passwords must be redefined. Select algorithms and a key storage method, and implement FIPS-compliant encryption immediately after installation, *before* you begin to work with the product.

https://support.ca.com/cadocs/0/CA%20GovernanceMinder%2012%206%201-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1150668.html

HOW TO UPDATE FIPS

Password Tool Syntax

This command has the following syntax:

```
pwdtools -[FIPSKEY|JSAFE|FIPS] -p [plain text] -k [key file location]
```

JSAFE

Encrypt a plain text value using non-FIPS algorithm.

Example:

```
pwdtools -JSAFE -p mypassword
```

FIPSKEY

Create a FIPS key file.

Example:

```
pwdtools -FIPSKEY -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the location where you want the FIPS key to be stored.

The password tool creates the FIPS key in the location specified.

Note: Be sure to secure the key by setting the directory access permissions for specific group or user types.

FIPS

Encrypt a plain text value using a FIPS key file. This uses the existing FIPS key file.

Example:

```
pwdtools -FIPS -p firewall -k C:\keypath\FIPSkey.dat
```

Where *keypath* is the full path to the FIPS key directory.

https://support.ca.com/cadocs/0/CA%20GovernanceMinder%2012%206%201-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1150668.html